IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

DAQUARIOUS ALEXANDER, on behalf of themselves and all others similarly situated, Plaintiff(s), vs. **LANSING COMMUNITY COLLEGE**, Defendant	Case No: **CLASS ACTION** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Daquarious Alexander individually and on behalf of all others similarly situated, brings this action against Defendant Lansing Community College, ("Defendant" or "LCC"). Plaintiff seeks to obtain damages, restitution, and injunctive relief for the Class, as defined below. Plaintiff makes the following allegations upon information and belief, except as to his own actions, the investigation of his counsel, and the facts that are a matter of public record.

INTRODUCTION

1. This class action arises out of the recent targeted cyberattack and data breach on LCC's network that resulted in unauthorized access of highly sensitive data. Plaintiff brings this class action against LCC for its failure to secure and safeguard approximately 757,832 individuals' personally identifiable information ("PII"). As a result, Plaintiff and Class Members suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack, emotional distress, and the imminent risk of future harm caused by the compromise of their sensitive personal information.

2. Lansing Community College is an institution of higher education located in Lansing, Michigan. LCC is one of the largest community colleges in Michigan, enrolling approximately 17,700 students annually.[1]

3. According to LCC, the highly sensitive personally identifiable information that was subject to "unauthorized access" in the Data Breach included names and Social Security numbers (collectively "PII").

4. On or around March 14, 2023, LCC became aware of suspicious activity on its computer network. LCC launched an investigation, revealing that, between December 25, 2022 and March 15, 2023, an "unauthorized actor" may have had access to its systems.[2] LCC has since confirmed that there were 757,835 people impacted by the Data Breach.[3]

5. The Data Breach was a direct result of LCC's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect consumers' PII. By taking possession and control of Plaintiff's and Class Members' PII for its own pecuniary benefit, LCC assumed a duty to Plaintiff and Class Members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard Plaintiff's and Class Members' PII against unauthorized access and disclosure. LCC also had a duty to adequately safeguard this PII under industry standards and duties imposed by statutes, including Section 5 of the Federal Trade Commission Act ("FTC Act"). LCC breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect Plaintiff's and other individuals' PII from unauthorized access and disclosure.

---

[1] Lansing Community College, https://www.lcc.edu/about/ (last visited July 6, 2023).
[2] Yahoo!Finance, https://finance.yahoo.com/news/lansing-community-college-lcc-notice-210000106.html? (last visited July 6, 2023).
[3] https://apps.web.maine.gov/online/aeviewer/ME/40/9da7ece2-89a4-435a-916d-3ab465e03645.shtml (last visited July 8, 2023).

6. The exposure of a person's PII through a data breach ensures that such person will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of their lives. As a result of the Data Breach, Plaintiff and Class Members are at imminent and substantial risk of experiencing various types of misuse of their PII in the coming years, including but not limited to, unauthorized access to personal accounts, tax fraud, and identity theft.

7. Social Security numbers are particularly valuable to criminals. This information can be sold and traded on the "dark web" black market. The loss of a Social Security number is particularly troubling because it cannot be easily changed and can be misused in a range of nefarious activities, such as filing fraudulent tax returns to steal tax refund payments, opening new accounts to take out loans, and other forms of credit and identity theft.

8. Mitigating that risk, to the extent it is even possible to do so, requires individuals to devote significant time and money to closely monitor their credit, financial accounts, and email accounts, and take several additional prophylactic measures.

9. Plaintiff and Class Members may now incur out of pocket costs for purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft. They will also be forced to expend additional time to review credit reports and monitor their financial accounts for fraud or identity theft.

10. Plaintiff brings this Class Action Complaint for LCC's failure to comply with industry standards to protect their information systems that contain PII and Defendant's failure to provide timely and adequate notice to Plaintiff and other Class Members that their PII had been compromised.

11. Plaintiff, individually and all others similarly situated, bring claims for negligence; negligence *per se*; breach of fiduciary duty; unjust enrichment; breach of implied contract; and violation of the Michigan Consumer Protection Act, Mich. Comp. Laws Ann § 445.901, *et. seq.*

PARTIES

A. Plaintiff

12. Plaintiff Daquarious Alexander is a resident and citizen of the State of Michigan. The Plaintiff was a part of LCC's Lansing Promise program, which allowed LCC access to Plaintiff's PII.

13. Plaintiff Alexander subsequently received a notice letter from LCC on or around June 30, 2023, informing him that his PII was impacted by LCC's Data Breach.

14. As a direct and proximate result of the Data Breach, and in addition to the injuries alleged herein, Plaintiff Alexander spent significant time dealing with the potential effects of the Data Breach. The time spent dealing with these incidents resulting from the Data Breach is time the Plaintiff otherwise would have spent on other activities, such as work and/or recreation.

15. Plaintiff Alexander plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his accounts for any unauthorized activity.

B. Defendant

16. Defendant Lansing Community College is an entity with its principal place of business at 600 N. Grand Avenue, Lansing, MI 48933.

JURISDICTION AND VENUE

17. This Court has subject matter jurisdiction over this controversy pursuant to 28 U.S.C. § 1332(d). The amount in controversy in this class action exceeds $5,000,000, exclusive of interest and costs, and there are numerous Class Members who are citizens of states other than Defendant's state of citizenship.

18. This Court has personal jurisdiction over LCC because it is authorized to and does conduct substantial business in this District and is a citizen of this District by virtue of its principal place of business being located in this District.

19. Venue is proper in this District, pursuant to 28 U.S.C. § 1391(b), because a substantial part of the acts, omissions, and events giving rise to Plaintiff's claims occurred in Ingham County, which is in this District.

FACTUAL ALLEGATIONS

A. Background

20. As noted above, Defendant LCC is a community college. There are approximately17,700 students currently enrolled at LCC.[4]

21. Plaintiff and the Class Members, as current or former students, employees and vendors, reasonably relied (directly or indirectly) on this sophisticated higher education institution to keep their sensitive PII confidential; to maintain its system security; to use this information for business purposes only; and to make only authorized disclosures of their PII. Plaintiff and Class Members provided their PII to LCC with the reasonable expectation and mutual understanding that it would comply with its obligations to keep such information confidential and secure from unauthorized access.

[4] https://www.lcc.edu/about/ (last visited July 8, 2023).

22. LCC had a duty to adopt reasonable measures to protect Plaintiff's and Class Members' PII from involuntary disclosure to third parties. As evidenced by the Data Breach, it failed to adhere to that duty.

23. LCC's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches preceding the date it disclosed the incident.

B. The Data Breach and Notice Letter

24. The "Notice of Data Event" on LCC's website states that LCC first became aware of "suspicious activity on its computer network" on or around March 14, 2023.[5] Thereafter, it engaged "third-party computer specialists" to undertake an investigation.[6]

25. The investigation determined that, between December 25, 2022 and March 15, 2023, an unauthorized actor may have had access to certain systems.

26. While not disclosed on the school's website, LCC has advised the Maine Attorney General that Social Security numbers were compromised in the breach.[7]

27. LCC has also revealed in filings with the Maine Attorney General that it is offering "12 months of credit monitoring and identity restoration services through Kroll."[8] For the reasons discussed below, that period of time is woefully inadequate under the circumstances herein.

C. LCC Failed to Comply with FTC Guidelines

28. LCC was prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain

[5] https://www.lcc.edu/alert.html (last visited July 8, 2023).
[6] *Id.*
[7] https://apps.web.maine.gov/online/aeviewer/ME/40/9da7ece2-89a4-435a-916d-3ab465e03645.shtml (last visited July 8, 2023).
[8] *Id.*

reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

29. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

30. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[9] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach. *Id.*

31. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

---

[9] *See* ECF No. 1-27, *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016).

32. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

33. LCC failed to properly implement basic data security practices.

34. LCC's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

35. LCC was at all times fully aware of the obligation to protect the Private Information of Plaintiff and Class Members. LCC was also aware of the significant repercussions that would result from its failure to do so.

36. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice that violates the FTC Act.

D. LCC Failed to Comply with Data Security Industry Standards

37. As shown above, experts studying cybersecurity routinely identify colleges and universities being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain. For example, in December of 2022, Hope College announced that it had experienced a similar data breach that comprised Social Security numbers and other PII.[10] At the

[10] https://www.michigan.gov/ag/news/press-releases/2022/12/28/ag-urges-students-impacted-by-hope-college-data-breach-to-take-steps-to-protect-personal-information (last visited July 8, 2023).

time, Michigan Attorney General Dana Nessel issued a press release which stated that "Anyone who received notice from Hope College related to this breach should be taking steps to combat potential identify theft."[11]

38. LCC is aware of the importance of safeguarding Plaintiff's and Class Members' PII, that by virtue of their business—as a higher education institution—they place Plaintiff's and Class Members' PII at risk of being targeted by cybercriminals.

39. Because LCC failed to implement, maintain, and comply with necessary cybersecurity requirements, as a result, it was unable to protect Plaintiff's and Class Members' information and confidentiality, and protect against obvious and readily foreseeable threats to information security and confidentiality.

40. As a proximate result of such failures, cybercriminals gained unauthorized access to Defendant's network and acquired Plaintiff's and Class Members' PII in the Data Breach without being stopped.

41. Defendant was unable to prevent the Data Breach and was unable to detect the unauthorized access to vast quantities of sensitive and protected files containing Plaintiff's and Class Members' PII.

42. Commonly accepted data security standards among businesses and higher education institutions that store personal information, such as the PII involved here, include, but are not limited to:

[11] *Id.*

a. Maintaining a secure firewall configuration;

b. Monitoring for suspicious or irregular traffic to servers;

c. Monitoring for suspicious credentials used to access servers;

d. Monitoring for suspicious or irregular activity by known users;

e. Monitoring for suspicious or unknown users;

f. Monitoring for suspicious or irregular server requests;

g. Monitoring for server requests for personal and financial information;

h. Monitoring for server requests from VPNs; and

i. Monitoring for server requests from Tor exit nodes.

43. The U.S. Federal Trade Commission ("FTC") publishes guides for businesses for Cybersecurity (*Start with Security: A Guide for Business*, (June 2015)) and protection of personal and financial information (Protecting *Personal Information: A Guide for Business*, (Oct. 2016)), which includes basic security standards applicable to all types of businesses and higher education institutions.

44. The FTC has *brought* enforcement actions against businesses for failing to adequately and reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses and higher education institutions must take to meet their data security obligations.

45. Because Defendant was entrusted with Plaintiff's and Class Members' PII, they had and have a duty to keep the PII secure.

46. Plaintiff and Class Members reasonably expect that when they entrusted their PII to LCC it will safeguard their information.

47. Despite Defendant's obligations, Defendant failed to appropriately monitor and maintain their data security systems in a meaningful way so as to prevent the Data Breach.

48. Had Defendant properly maintained their systems and adequately protected them, they could have prevented the Data Breach.

E. LCC Violated its Common Law Duty of Reasonable Care

49. LCC was aware of the importance of security in maintaining personal information (particularly sensitive personal information like the PII involved here), and the value consumers place on keeping their PII secure.

50. In addition to obligations imposed by federal and state law, Defendant owed and continues to owe a common law duty to Plaintiff and Class Members—who entrusted Defendant with their PII—to exercise reasonable care in receiving, maintaining, and storing, the PII in Defendant's possession.

51. Defendant owed and continues to owe a duty to prevent Plaintiff's and Class Members' PII from being compromised, lost, stolen, accessed, or misused by unauthorized third parties. An essential part of Defendant's duty was (and is) the obligation to provide reasonable security consistent with current industry best practices and requirements, and to ensure information technology systems and networks, in addition to the personnel responsible for those systems and networks, adequately protected and continue to protect Plaintiff's and Class Members' PII.

52. Defendant owed a duty to Plaintiff and Class Members, who entrusted Defendant with extremely sensitive PII to design, maintain, and test the information technology systems that

housed Plaintiff's and Class Members' PII, to ensure that the PII in Defendant's possession was adequately secured and protected.

53. Defendant owed a duty to Plaintiff and Class Members to create, implement, and maintain reasonable data security practices and procedures sufficient to protect the PII stored in Defendant's systems. In addition, this duty also required LCC to adequately train its employees and others with access to Plaintiff's and Class Members' PII on the procedures and practices necessary to safeguard such sensitive information. This duty also required supervision, training, and compliance on LCC's part to ensure that it complied with creating, implementing, and maintaining reasonable data security practices and procedures sufficient to protect Plaintiff's and Class Members' PII.

54. Defendant owed a duty to Plaintiff and Class Members to implement processes that would enable Defendant to timely detect a breach of its information technology systems, and a duty to act upon any data security warnings or red flags detected by such systems in a timely fashion.

55. Defendant owed a duty to Plaintiff and Class Members to disclose when and if their information technology systems and data security practices were not sufficiently adequate to protect and safeguard Plaintiff's and Class Members' PII.

56. Thus, Defendant owed a duty to Plaintiff and Class Members to timely disclose the fact that a data breach, resulting in unauthorized access to their PII, had occurred.

57. Defendant violated these duties. The Notice Letter further states that LCC became aware of the Data Breach on March 14, 2023, however Plaintiff and Class Members, and the public did not learn of the Data Breach until June 30, 2023, when the Notice Letters were mailed out. Defendant failed to publicly describe the full extent of the Data Breach and notify affected parties.

This demonstrates that LCC did not properly implement measures designed to timely detect a data breach of their information technology systems, as required to adequately safeguard Plaintiff's and Class Members' PII.

58. Defendant also violated their duty to create, implement, and maintain reasonable data security practices and procedures sufficient to protect Plaintiff's and Class Members' PII.

59. LCC breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. LCC's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

- Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;
- Failing to adequately protect customers' PII;
- Failing to properly monitor its own data security systems for existing intrusions;
- Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures;
- Failing to detect unauthorized ingress into its systems;
- Failing to implement and monitor reasonable network segmentation to detect unauthorized travel within its systems, including to and from areas containing the most sensitive data;
- Failing to detect unauthorized exfiltration of the most sensitive data on its systems;
- Failing to train its employees in the proper handling of emails containing PII and maintain adequate email security practices;
- Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act;
- Failing to adhere to industry standards for cybersecurity as discussed above; and

- Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' Private PII.

60. LCC negligently and unlawfully failed to safeguard Plaintiff's and Class Members PII by allowing cybercriminals to access its computer network which contained unsecured and unencrypted PII.

61. Had LCC remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, LCC could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential PII.

62. However, due to LCC's failures, Plaintiff and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiff and the Class Members also lost the benefit of the bargain they made with LCC.

F. LCC Knew or Should Have Known That Criminals Target PII and the Data Breach Was Foreseeable and Preventable

63. Defendant was well aware that the protected PII it acquires, stores, and utilizes is highly sensitive and of significant value to the owners of the PII and those who would use it for wrongful purposes.

64. PII is a valuable commodity to identity thieves, particularly when it is aggregated in large numbers. Former United States Attorney General William P. Barr made clear that consumers' sensitive personal information commonly stolen in data breaches "has economic value." The purpose of stealing large caches of personal data is to use it to defraud individuals or to place it for illegal sale and to profit from other criminals who buy the data and use it to commit fraud and identity theft. Indeed, cybercriminals routinely post stolen personal information on anonymous websites, making the information widely available to the criminal underworld.

65. There is an active and robust market for this information. As John Sancenito, president of *Information Network* Associates, a company which helps companies with recovery after data breaches, explained after a data breach "[m]ost of the time what [data breach hackers] do is they steal the data and then they sell the data on the dark web to the people who actually commit the fraud."

66. PII is a valuable property right.[12] The value of Private Information as a commodity is measurable.[13] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[14] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[15] Private Information is so valuable to identity thieves that once Private Information has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

67. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, SSNs, PII, and other sensitive information directly on various Internet websites, making the information publicly available. This

---

[12] *See* Marc van Lieshout, *The Value of Personal Data*, 457 IFIP ADVANCES IN INFORMATION AND COMMUNICATION TECHNOLOGY 26 (May 2015), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible[.]") (last visited July 6, 2023).

[13] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE (Apr. 28, 2014), http://www.medscape.com/viewarticle/824192 (last visited July 6, 2023).

[14] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD 4 (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en (last visited July 6, 2023).

[15] *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/ (last visited Feb. 24, 2023).

information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

68. The forms of PII involved in this Data Breach are particularly concerning and are a prime target for cybercriminals.

69. ***Social Security numbers***—Unlike credit or debit card numbers in a payment card data breach—which can quickly be frozen and reissued in the aftermath of a breach—unique Social Security numbers cannot be easily replaced. Even when such numbers are replaced, the process of doing so results in a major inconvenience to the subject person, requiring a wholesale review of the person's relationships with government agencies and any number of private companies in order to update the person's accounts with those entities.

70. Indeed, even the Social Security Administration warns that the process of replacing a Social Security number is a difficult one that creates other types of problems, and that it will not be a panacea for the affected person:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with

> your new number, the absence of any credit history under the new number may make more difficult for you to get credit.

71. Social Security numbers allow individuals to apply for credit cards, student loans, mortgages, and other lines of credit—among other services. Often Social Security numbers can be used to obtain goods or services. They are also used to apply for a host of government benefits. Access to such a wide range of assets makes Social Security numbers a prime target for cybercriminals and a particularly attractive form of PII to steal and then sell.

72. The ramifications of Defendant's failure to keep Plaintiff's and Class Members' PII secure are long lasting and severe. To avoid detection, identity thieves often hold stolen data for months or years before using it. Also, the sale of stolen information on the "dark web" may take months or more to reach end-users, in part because the data is often sold in small batches as opposed to in bulk to a single buyer. Thus, Plaintiff and Class Members must vigilantly monitor their accounts *ad infinitum*.

73. Thus, Defendant knew, or should have known, the importance of safeguarding the PII entrusted to it and of the foreseeable consequences if its systems were breached. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

74. As a highly sophisticated party that handles sensitive PII, Defendant failed to establish and/or implement appropriate administrative, technical and/or physical safeguards to ensure the security and confidentiality of Plaintiff's and other Class Members' PII to protect against anticipated threats of intrusion of such information.

75. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud. According to Experian, one of the largest credit reporting companies in the world, "[t]he research

shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan, change a billing address so the victim no longer receives bills, open new utilities, obtain a mobile phone, open a bank account and write bad checks, use a debit card number to withdraw funds, obtain a new driver's license or ID, and/or use the victim's information in the event of arrest or court action.

76. Identity thieves can also use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, and/or rent a house or receive medical services in the victim's name.

77. Moreover, theft of Private Information is also gravely serious because Private Information is an extremely valuable property right.[16]

78. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

79. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

80. The PII exfiltrated in the Data Breach can also be used to commit identity theft by placing Plaintiff and Class Members at a higher risk of "phishing," "vishing," "smishing," and "pharming," which are which are other ways for cybercriminals to exploit information they already have in order to get even more personally identifying information from a person through

[16] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted) (last accessed July 6, 2023).

unsolicited email, text messages, and telephone calls purportedly from a legitimate company requesting personal, financial, and/or login credentials.

81. There is often a lag time between when fraud occurs versus when it is discovered, as well as between when PII is stolen and when it is used. According to the *U.S. Government Accountability Office*, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

82. Personal information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the cyber black market for years. Indeed, a social security number, date of birth, and full name can sell for $60 to $80 on the digital black market[17]. "[I]f there is reason to believe that your personal information has been stolen, you should assume that it can end up for sale on the dark web."[18]

83. Plaintiff and Class Members rightfully place a high value not only on their PII, but also on the privacy of that data.

84. Thus, Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future. These risks are both certainly impending and substantial. As the FTC has reported, if hackers get access to PII, they *will use it.*

---

[17] Michael Kan, *Here's How Much Your Identity Goes for on the Dark Web*, Nov. 15, 2017, https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web (last accessed July 6, 2023).

[18] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America, Mar. 19, 2019, https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/ (last accessed July 6, 2023).

85. Data breaches are preventable. As Lucy Thompson wrote in the *Data Breach and Encryption Handbook*, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions." She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised…" and "[m]ost of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures…Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a data breach never occurs."

86. The types of PII, such as Social Security and driver's license numbers, compromised in the Data Breach are immutable. Plaintiff and Class Members are not able to change them or simply cancel them, like a credit card, to avoid harm or fraudulent use of the information. Just like a birthdate or a mother's maiden name, these pieces of information cannot be changed by logging into a website and changing them in settings, and they can be used alone or in conjunction with other pieces of Plaintiff's and Class Members' information to commit serious identity theft and fraud.

87. The Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. *Id.* at 4. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's

employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

88. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[19]

89. This was a financially motivated Data Breach, as the only reason the cybercriminals go through the trouble of running a targeted cyberattack against entities like LCC is to get information that they can monetize by selling on the black market for use in the kinds of criminal activity described herein. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."

90. It is within this context that Plaintiff and all other Class Members must now live with the knowledge that their Private Information is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black market.

[19] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/ (emphasis added) (last accessed July 6, 2023).

91. Victims of the Data Breach, like Plaintiff and Class Members, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their privacy and credit because of the Data Breach.

92. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have had their PII exposed, have suffered harm as a result, and have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiff and Class Members must now take the time and effort (and spend the money) to mitigate the actual and potential impact of the Data Breach on their everyday lives, including purchasing identity theft and credit monitoring services every year for the rest of their lives, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, and credit reports for unauthorized activity for years to come.

G. Plaintiff and Class Members Suffered Harm as a Result of the Data Breach

93. The ramifications of Defendant's failure to keep PII secure are long-lasting and severe. Victims of data breaches are more likely to become victims of identity fraud, occurring 65 percent of the time. In 2019 alone, consumers lost more than $1.9 billion to identity theft and fraud.

94. Besides damage sustained in the event of identity theft, consumers may also spend anywhere from approximately 7 hours to upwards to over 1,000 hours trying to resolve identity theft issues. The Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems."

95. Plaintiff's and Class Members' PII was provided to LCC in conjunction with the type of work LCC performs as an educational institution. In requesting and maintaining Plaintiff's and Class Members' PII, LCC promised, and undertook a duty, to act reasonably in its handling of Plaintiff's and Class Members' PII. LCC, however, did not take proper care of Plaintiff's and Class Members' PII, leading to its exposure to and exfiltration by cybercriminals as a direct result of LCC's inadequate data security measures.

96. As a result of LCC's conduct and failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect consumers' PII, which allowed the Data Breach to occur, Plaintiff's and Class Members' PII has been and is now in the hands of unauthorized individuals and third parties, which may include thieves, unknown criminals, banks, credit companies, and other potentially hostile individuals.

97. Plaintiff and Class Members greatly value their privacy, especially their highly-sensitive information, such as their first and last names, dates of birth, Social Security numbers, and driver's license numbers. They would not have entrusted LCC with this highly-sensitive information, had they known that LCC would negligently fail to adequately protect their PII. Indeed, Plaintiff and Class Members provided LCC with this highly-sensitive information with the expectation that LCC would keep their PII secure and inaccessible from unauthorized parties.

98. As a result of LCC's failure to implement and follow even the most basic security procedures, Plaintiff and Class Members suffered actual damages including, without limitation, time and expenses related to monitoring their financial accounts for fraudulent activity, exposure to increased and imminent risk of fraud and identity theft, the loss in value of their personal information, and other economic and non-economic harm. Plaintiff and Class Members will now be forced to expend additional time to review their credit reports and monitor their financial

accounts and medical records for fraud or identify theft—particularly since the compromised information may include Social Security numbers.

99. Once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives.

100. Plaintiff and Class Members are also at a continued risk of harm because their PII remains in LCC's systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as LCC fails to undertake the necessary and appropriate data security measures to protect the PII in its possession.

101. As a result of the Data Breach, and in addition to the time Plaintiff and Class Members have spent and anticipate spending to mitigate the impact of the Data Breach on their lives, Plaintiff and Class Members have also suffered emotional distress from the public release of their PII, which they believed would be protected from unauthorized access and disclosure. The emotional distress they have experienced includes anxiety and stress resulting from the fear that unauthorized bad actors are viewing, selling, and or using their PII for the purposes of identity theft and fraud.

102. Additionally, Plaintiff and Class Members have suffered damage to and diminution in the value of their highly sensitive and confidential PII—a form of property that Plaintiff and Class Members entrusted to LCC and which was compromised as a result of the Data Breach LCC failed to prevent. Plaintiff and Class Members have also suffered a violation of their privacy rights as a result of LCC's unauthorized disclosure of their PII.

CLASS ACTION ALLEGATIONS

103. Plaintiff brings this case individually and, pursuant to Rule 23(b)(2), (b)(3), and (c)(4) of the Federal Rules of Civil Procedure, on behalf of the following Nationwide Class and state classes (collectively the "Class") (Michigan Classes are collectively referred to as the "State Classes"):

> **Nationwide Class**
> All persons whose PII was compromised in the Data Breach that was discovered by LCC on or around March 14, 2023.

In addition, or in the alternative, Plaintiff proposes the following state class:

> **Michigan Class**
> All residents of Michigan whose PII was compromised in the Data breach that was discovered by LCC on or around March 14, 2023.

104. Excluded from the Class is LCC, its subsidiaries and affiliates, its officers, directors and members of their immediate families and any entity in which LCC has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

105. Plaintiff reserves the right to modify or amend the definition of the proposed Class, if necessary, before this Court determines whether certification is appropriate.

106. The requirements of Rule 23(a)(1) are satisfied. The Class described above is so numerous that joinder of all individual members in one action would be impracticable. The disposition of the individual claims of the respective Class Members through this class action will benefit both the parties and this Court. As noted above, there are approximately 757,832 Class Members.

107. The exact size of the Class and the identities of the individual members thereof are ascertainable through Defendant's records, including but not limited to, the information implicated in the Data Breach.

108. The requirements of Rule 23(a)(2) are satisfied. There is a well-defined community of interest and there are common questions of fact and law affecting Class Members. The questions of fact and law common to the Class predominate over questions which may affect individual members and include the following:

a. Whether and to what extent Defendant had a duty to secure and protect the PII of Plaintiff and Class Members;

b. Whether Defendant were negligent in collecting and disclosing Plaintiff's and Class Members' PII;

c. Whether Defendant had duties not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;

d. Whether Defendant took reasonable steps and measures to safeguard Plaintiff's and Class Members' PII;

e. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members;

f. Whether Defendant breached their duties to exercise reasonable care in handling Plaintiff's and Class Members' PII in the manner alleged herein, including failing to comply with industry standards;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendant had respective duties not to use the PII of Plaintiff and Class Members for non-business purposes;

i. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

j. Whether Plaintiff and Class Members are entitled to declaratory judgment under 28 U.S.C. § 2201, *et seq.*;

k. Whether Plaintiff and Class Members are entitled to damages as a result of Defendant's wrongful conduct; and

l. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

109. The requirements of Rule 23(a)(3) are satisfied. Plaintiff's claims are typical of the claims of Class Members. The claims of the Plaintiff and Class Members are based on the same legal theories and arise from the same failure by Defendant to safeguard PII. Plaintiff and Class Members each had their PII disclosed by Defendant to an unauthorized third party.

110. The requirements of Rule 23(a)(4) are satisfied. Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the Class Members. Plaintiff will fairly, adequately, and vigorously represent and protect the interests of Class Members and have no interests antagonistic to the Class Members. In addition, Plaintiff has retained counsel who are competent and experienced in the prosecution of class action litigation, including data breach litigation. The claims of Plaintiff and Class Members are substantially identical as explained above. While the aggregate damages that may be awarded to the Class Members are likely to be substantial, the damages suffered by the individual Class Members are

relatively small. As a result, the expense and burden of individual litigation make it economically infeasible and procedurally impracticable for each member of the Class to individually seek redress for the wrongs done to them. Certifying the case as a class will centralize these substantially identical claims in a single proceeding, which is the most manageable litigation method available to Plaintiff and the Class and will conserve the resources of the parties and the court system, while protecting the rights of each member of the Class. Defendant's uniform conduct is generally applicable to the Class as a whole, making relief appropriate with respect to each Class Member.

111. Here a class action is superior to other available methods for the fair and efficient adjudication of this controversy. The adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudications of the asserted claims. There will be no difficulty in managing this action as a class action, and the disposition of the claims of the Class members in a single action will provide substantial benefits to all parties and to the Court. Damages for any individual Class Member are likely insufficient to justify the cost of individual litigation so that, in the absence of class treatment, Defendant's violations of law inflicting damages in the aggregate would go un-remedied.

112. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and the Classes to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendant's data security practices were reasonable in light of best practices recommended by data security experts;

c. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

d. Whether Defendant failed to take commercially reasonable steps to safeguard consumer PII; and

e. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

113. Finally, all members of the proposed Classes are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. At least some Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, the Michigan Class)

114. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

115. LCC owed a duty to Plaintiff and all other Class Members to exercise reasonable care in safeguarding and protecting their PII in its possession, custody, or control.

116. LCC knew, or should have known, the risks of collecting and storing Plaintiff's and all other Class Members' PII and the importance of maintaining secure systems. LCC knew, or should have known, of the vast uptick in data breaches in recent years. LCC had a duty to protect the PII of Plaintiff and Class Members.

117. Given the nature of LCC's business, the sensitivity and value of the PII it maintains, and the resources at its disposal, LCC should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring, which LCC had a duty to prevent.

118. LCC breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII entrusted to it—including Plaintiff's and Class Members' PII.

119. It was reasonably foreseeable to LCC that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class Members' PII to unauthorized individuals.

120. But for LCC's negligent conduct/breach of the above-described duties owed to Plaintiff and Class Members, their PII would not have been compromised.

121. As a result of LCC's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and all other Class Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and

international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vii) actual or attempted fraud.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Nationwide Class, or Alternatively, the Michigan Class)

122. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

123. In addition to the common law, LCC's duties arise from Section 5 of the FTCA ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by a business, such as LCC, of failing to employ reasonable measures to protect and secure PII.

124. LCC violated Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and all other Class Members' PII and not complying with applicable industry standards. LCC's conduct was particularly unreasonable given the nature and amount of PII it obtains and stores, and the foreseeable consequences of a data breach involving PII including, specifically, the substantial damages that would result to Plaintiff and the other Class Members.

125. LCC's violations of Section 5 of the FTCA constitutes negligence *per se*.

126. Plaintiff and Class Members are within the class of persons that Section 5 of the FTCA was intended to protect.

127. The harm occurring as a result of the Data Breach is the type of harm Section 5 of the FTCA was intended to guard against.

128. It was reasonably foreseeable to LCC that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII by failing to design, adopt,

implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class Members' PII to unauthorized individuals.

129. The injury and harm that Plaintiff and the other Class Members suffered was the direct and proximate result of LCC's violations of Section 5 of the FTCA. Plaintiff and Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vi) actual or attempted fraud.

COUNT III
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, the Michigan Class)

130. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

131. Plaintiff and Class Members either directly or indirectly gave LCC their PII in confidence, believing that LCC – a private college – would protect that information. Plaintiff and Class Members would not have provided LCC with this information had they known it would not be adequately protected. LCC's acceptance and storage of Plaintiff's and Class Members' PII created a fiduciary relationship between LCC and Plaintiff and Class Members. In light of this

relationship, LCC must act primarily for the benefit of its customers and students (at least insofar as it relates to the safeguarding of their PII).

132. LCC has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their relationship. It breached that duty by failing to properly protect the integrity of the system containing Plaintiff's and Class Members' PII, failing to comply with the data security guidelines set forth by Section 5 of the FTCA, and otherwise failing to safeguard the PII of Plaintiff and Class Members it collected.

133. As a direct and proximate result of LCC's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII which remains in LCC's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII compromised as a result of the Data Breach; and (vii) actual or attempted fraud.

COUNT IV
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, the Michigan Class)

134. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein. This claim is pled in the alternative to the implied contract claim pursuant to Fed. R. Civ. P. 8(d)(2).

135. Plaintiff and Class Members conferred a monetary benefit upon LCC in the form of monies paid for educational services or other services.

136. LCC accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class Members. LCC also benefited from the receipt of Plaintiff's and Class Members' PII.

137. As a result of LCC's conduct, Plaintiff and Class Members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiff and Class Members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

138. LCC should not be permitted to retain the money belonging to Plaintiff and Class Members because LCC failed to adequately implement the data privacy and security procedures for itself that Plaintiff and Class Members paid for and that were otherwise mandated by federal, state, and local laws. and industry standards.

139. LCC should be compelled to provide for the benefit of Plaintiff and Class Members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

COUNT V
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, the Michigan Class)

140. Plaintiff reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

141. Defendant required Plaintiff and Class Members to provide, or authorize the transfer of, their PII in order for LCC to provide educational services and employment. In exchange, LCC entered into implied contracts with Plaintiff and Class Members in which LCC agreed to comply with its statutory and common law duties to protect Plaintiff's and Class Members' PII and to timely notify them in the event of a data breach.

142. Plaintiff and Class Members would not have provided their PII to Defendant had they known that Defendant would not safeguard their PII, as promised, or provide timely notice of a data breach.

143. Plaintiff and Class Members fully performed their obligations under their implied contracts with Defendant.

144. Defendant breached the implied contracts by failing to safeguard Plaintiff's and Class Members' PII and by failing to provide them with timely and accurate notice of the Data Breach.

145. The losses and damages Plaintiff and Class Members sustained (as described above) were the direct and proximate result of Defendant's breach of its implied contracts with Plaintiff and Class Members.

COUNT VI
MICHIGAN CONSUMER PROTECTION ACT
(Mich. Comp. Laws Ann §§ 445.901, *et. seq.*)
(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, the Michigan Class)

146. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

147. The Michigan Consumer Protection Act was created to protect Michigan consumers from unfair, unconscionable, or deceptive methods, acts, or practices in the conduct of trade or commerce.

148. Plaintiff and Class Members provided PII to Defendant pursuant to transactions (i.e., providing education) they engaged in with Defendant as customers and students.

149. Defendant has its principal place of business and headquarters in Michigan and transacts with Michigan consumers and students.

150. LCC engaged in deceptive trade practices in the conduct of its business, in violation of Mich. Comp. Laws Ann § 445.901, including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

151. LCC's deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' PII, including duties

imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' PII, including duties imposed by the FTCA, 15 U.S.C. § 45, and

f. Failing to timely and adequately notify Plaintiff, and Class Members of the Data Breach;

g. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class Members' PII; and

h. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class Members' PII, including duties imposed by the FTCA, 15 U.S.C. § 45.

152. LCC's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of LCC's data security and ability to protect the confidentiality of consumers' PII.

153. LCC's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiff and the Class Members, that their PII was not exposed and misled Plaintiff and the Class Members into believing they did not need to take actions to secure their identities.

154. LCC intended to mislead Plaintiff and Class Members and induce them to rely on its misrepresentations and omissions.

155. Had LCC disclosed to Plaintiff and Class Members that its data systems were not secure and, thus, vulnerable to attack, LCC would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, LCC was trusted with sensitive and valuable PII regarding hundreds of thousands of consumers, including Plaintiff, and the Michigan Subclass. LCC accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because LCC held itself out as maintaining a secure platform for PII data, Plaintiff and the Class Members acted reasonably in relying on LCC's misrepresentations and omissions, the truth of which they could not have discovered.

156. As a direct and proximate result of LCC's deceptive trade practices, Plaintiff and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII.

157. Plaintiff and Class Members are likely to be damaged by LCC's ongoing deceptive trade practices.

158. Plaintiff and the Class Members seek all monetary and non-monetary relief allowed by law, including damages or restitution, injunctive or other equitable relief, and attorneys' fees and costs.

159. Accordingly, pursuant to Mich. Comp. Law Ann. § 445.901, *et seq.*, Michigan Plaintiff and Class members are entitled to recover their actual damages, which can be calculated

with a reasonable degree of certainty using sufficiently definitive and objective evidence. Those damages are: (a) damage to and diminution in the value of their PII, a form of property that Defendant obtained from Plaintiff and Class Members; (b) violation of Plaintiff's and Class Members' privacy rights; (c) present and increased risk arising from the identity theft and fraud.; and other miscellaneous incidental and consequential damages. In addition, given the nature of LCC's conduct, Plaintiff and Class Members are entitled to all available statutory, exemplary, treble, and/or punitive damages and attorneys' fees based on the amount of time reasonably expended and equitable relief necessary or proper to protect them from LCC's unlawful conduct.

COUNT VII
VIOLATION OF THE MICHIGAN IDENTITY THEFT PROTECTION ACT
Mich. Comp. Laws Ann. §§ 445.72, *et seq.*
(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, the Michigan Class)

160. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

161. Defendant is a business that owns or licenses computerized data that includes PII as defined by Mich. Comp. Laws Ann. § 445.72(1).

162. Plaintiff's and Class Members' personal information (for the purpose of this count, "PII"), (e.g., Social Security numbers) includes PII as covered under Mich. Comp. Laws Ann. § 445.72(1).

163. Defendant is required to accurately notify Plaintiff and Class Members if it discovers a security breach or receives notice of a security breach (where unencrypted and unredacted PII was accessed or acquired by unauthorized persons), without unreasonable delay under Mich. Comp. Laws Ann. § 445.72(1).

164. Because Defendant discovered a security breach and had notice of a security breach, Defendant had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Mich. Comp. Laws Ann. § 445.72(4).

165. By failing to disclose the Data Breach in a timely and accurate manner, Defendant violated Mich. Comp. Laws Ann. § 445.72(4).

166. As a direct and proximate result of Defendant's violations of Mich. Comp. Laws Ann. § 445.72(4), Plaintiff and Class Members suffered damages, as described above.

167. Plaintiff and Class Members seek relief under Mich. Comp. Laws Ann. § 445.72(13), including a civil fine.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff on behalf of himself and all others similarly situated, prays for relief as follows:

(a) For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

(b) For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

(c) For damages, including all compensatory, punitive, and/or nominal damages, in an amount to be determined by the trier of fact;

(d) For an order of restitution and all other forms of equitable monetary relief;

(e) Declaratory and injunctive relief as described herein;

(f) Awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses;

(g) Awarding pre- and post-judgment interest on any amounts awarded; and

(h) Awarding such other and further relief as may be just and proper.

JURY TRIAL DEMAND

A jury trial is demanded on all claims so triable.

Dated: July 11, 2023

Respectfully submitted,

/s/ E. Powell Miller
E. Powell Miller (P39487)
Emily E. Hughes (P68724)
THE MILLER LAW FIRM, P.C.
950 W. University Dr., Suite 300
Rochester, MI 48307
T: (248) 841-2200
epm@millerlawpc.com
ssa@millerlawpc.com
eeh@millerlawpc.com

SHUB & JOHNS LLC
Jonathan Shub*
Benjamin F. Johns*
Samantha E. Holbrook*
Four Tower Bridge
200 Barr Harbor Drive, Suite 400
Conshohocken, PA 19428
(610) 477-8380
bjohns@shublawyers.com
sholbrook@shublawyers.com

**pro hac vice* application forthcoming

Attorneys for Plaintiff and the Putative Class